Arbitrary Precision Arithmetic

Robert C. Seacord, Software Engineering Institute [vita[1]]

2005-09-27; Updated 2008-10-06

L2 / D/P, L[2]

There are many arbitrary precision arithmetic packages available, primarily for scientific computing. However, arbitrary precision arithmetic can solve the problem of integer type range errors resulting from a lack of precision in the representation.

Development Context

Integer operations

Technology Context

C, C++, IA-32, Win32, UNIX

Attacks

Attacker executes arbitrary code on machine with permissions of compromised process or changes the behavior of the program.

Risk

Integers in C and C++ are susceptible to overflow, sign, and truncation errors that can lead to exploitable vulnerabilities.

Description

There are many arbitrary precision arithmetic packages available, primarily for scientific computing. However, they can also solve the problem of integer type range errors resulting from a lack of precision in the representation.

GNU Multiple Precision Arithmetic Library (GMP)

GMP is a portable library written in C for arbitrary precision arithmetic on integers, rational numbers, and floating-point numbers. It was designed to provide the fastest possible arithmetic for applications that require higher precision than what is directly supported by the basic C types.

GMP emphasizes speed over simplicity or elegance. It uses sophisticated algorithms, full words as the basic arithmetic type, and carefully optimized assembly code.

The GNU multiple precision library is licensed under the Lesser General Public License version 2.1 that accompanies the source code.

Java BigInteger

Newer versions of the Java JDK contain a BigInteger class in the java.math package. It provides arbitrary-precision integers, as well as analogs to all of Java’s primitive integer operators. While this does little for C and C++ programmers, it does illustrate that the concept is not entirely foreign to language designers.

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/274-BSI.html (Seacord, Robert C.)

Pearson Education, Inc. Copyright